A Thesis for the Degree of Ph.D. in Engineering

Implementation and Evaluation of Secured Network Infrastructure Using Content-based Router

February 2019

Graduate School of Science and Technology
Keio University

Rajitha L. TENNEKOON

別表６
（３）

Keio University

Thesis Abstract

No. 1

Registration Number	■ “KOU” □ “OTSU” No. *Office use only	Name	TENNEKOON RAJITHA LAKMAL

Thesis Title

Implementation and Evaluation of Secured Network Infrastructure Using Content-based Router

Thesis Summary

The Internet is the world’s largest public network accessed by approximately half of the world population. In principle, the Internet is used as the main communication medium, which aims to transfer all kinds of user and application data. Most of the time, users need to share their sensitive and private information along the communication with the authorized communication parties. As a public network, the Internet is constantly vulnerable by the miscellaneous threats and attacks such as malware, phishing, spoofing, injections, Denial-of-Service, ransomware, and hacking, which cause the exposure of the users’ private and sensitive information. These vulnerabilities have raised the demand for enhancing the functions of the Internet infrastructure to preserve confidentiality, integrity, and authentication (CIA) of their data.

The Internet use “TCP/IP” as its core communication protocol stack. The initial design of the Internet was intended to share data among networks with limited functionality. Such limitations of the core layer led to the inability to address the emerging security threats on its own. Such problems of the Internet ended up in allowing intruders to read and alter data streams. Moreover, it exposed the metadata used for the communication: i.e., packet header information. Therefore, over the past few decades, numerous studies have been conducted to study secure data transmission over public networks such as end-to-end data encryption (E2EE) protocols and tunneling protocols. Generally, a packet traverse through numerous networks between different countries among its delivery. It is a well-known fact that the security policies and requirements diverge among countries and organizations. However, the conventional methods secure data from one end to another without considering the connections in-between. Therefore, the used encryption algorithms or the keyspaces can be vulnerable among some of the intermediary links. On the contrary, tunneling encryption protocols are entirely independent of the routing flow; when data is encrypted or obscured by tunneling, it impedes analysis of traffic streams, which is the vital feature for the service-based future Internet. Moreover, it is vital to securely locate and track the adversary as early as possible after or during a network attack. However, lack of proper faster and secure traceability services is a major issue for the internet infrastructure and its users.

To this end, the dissertation proposes an approach to enhance the security over the public network communication using content-based router infrastructure. Content-based router is a next-generation novel backbone router, which can be used to analyze all packet stream transactions on its interfaces and provide extended services to end users and applications. On the contrary, the conventional routers

Thesis Abstract

cannot provide such services. Content-based routers use its specialized hardware and software modules to accelerate the packet processing and its services. The dissertation proposes an infrastructure to provide secured services using a novel distributed link-state routing (DLSR) protocol empowered with per-hop data encryption using the content-based router architecture. The implemented per-hop data encryption protocol is then used to provide mainly three services as the solutions for the above mention security issues, namely, 1) IP-routable entire packet encryption service, 2) neighbor data retransmission service and 3) fast and secure packet traceability service. Moreover, a core system for real-world content-based routers, named as deep packet inspector on a router (DooR), is implemented and tested which can perform on-the-fly TCP stream reconstruction and analysis leveraging the real-time deep packet inspection capabilities of the content-based routers.

Accordingly, the structure of the dissertation is divided into three main sections: 1) implement and evaluate per-hop data encryption protocol, 2) use the developed encryption protocol to provide secured services for public networks using content-based routers 3) leverages the content-based router infrastructure with hardware and software acceleration of DooR. The first two sections are implemented and evaluated under simulation-based environment using network simulator3 (ns-3). The DooR is implemented on real-world Linux-based high-performance hardware and tested in real-world networks. In conclusion, the proposed secured services yield better performance compared to the conventional methods together with better, flexible security to its users and the real-world DooR implementation guarantees the practicality of the proposed services via its hardware and software accelerations minimizing the packet processing delays in the content-based routers.